



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/457,732	12/10/1999	ANDREA CALIFANO	YO999-137	8003
21254	7590	10/02/2003	EXAMINER	
MCGINN & GIBB, PLLC 8321 OLD COURTHOUSE ROAD SUITE 200 VIENNA, VA 22182-3817			LAFORGIA, CHRISTIAN A	
			ART UNIT	PAPER NUMBER
			2131	

DATE MAILED: 10/02/2003

S

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/457,732

Applicant(s)

CALIFANO ET AL.

Examiner

Christian La Forgia

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 12 July 2002.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-36 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-36 is/are rejected.
- 7) ☒ Claim(s) 2,3,25 and 34 is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 14 February 2000 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- 11) ☐ The proposed drawing correction filed on _____ is: a) ☐ approved b) ☐ disapproved by the Examiner.
If approved, corrected drawings are required in reply to this Office action.
- 12) ☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

- 13) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
* See the attached detailed Office action for a list of the certified copies not received.
- 14) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).
a) ☐ The translation of the foreign language provisional application has been received.
- 15) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892) 4) ☐ Interview Summary (PTO-413) Paper No(s). _____
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948) 5) ☐ Notice of Informal Patent Application (PTO-152)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) 3. 6) ☐ Other: _____

Art Unit: 2131

DETAILED ACTION

1. Claims 1 through 36 are presented for examination.

Drawings

2. The drawings were received on 14 February 2000. These drawings are accepted by the Examiner.

3. The Patent and Trademark Office no longer makes drawing changes. See 1017 O.G. 4.

It is applicant's responsibility to ensure that the drawings are corrected. Corrections must be made in accordance with the instructions below.

INFORMATION ON HOW TO EFFECT DRAWING CHANGES

Replacement Drawing Sheets

Drawing changes must be made by presenting replacement figures which incorporate the desired changes and which comply with 37 CFR 1.84. An explanation of the changes made must be presented either in the drawing amendments, or remarks, section of the amendment. Any replacement drawing sheet must be identified in the top margin as "Replacement Sheet" and include all of the figures appearing on the immediate prior version of the sheet, even though only one figure may be amended. The figure or figure number of the amended drawing(s) must not be labeled as "amended." If the changes to the drawing figure(s) are not accepted by the examiner, applicant will be notified of any required corrective action in the next Office action. No further drawing submission will be required, unless applicant is notified.

Identifying indicia, if provided, should include the title of the invention, inventor's name, and application number, or docket number (if any) if an application number has not been assigned to the application. If this information is provided, it must be placed on the front of each sheet and centered within the top margin.

Annotated Drawing Sheets

A marked-up copy of any amended drawing figure, including annotations indicating the changes made, may be submitted or required by the examiner. The annotated drawing sheets must be clearly labeled as "Annotated Marked-up Drawings" and accompany the replacement sheets.

Timing of Corrections

Art Unit: 2131

Applicant is required to submit acceptable corrected drawings within the time period set in the Office action. See 37 CFR 1.85(a). Failure to take corrective action within the set period will result in ABANDONMENT of the application.

If corrected drawings are required in a Notice of Allowability (PTOL-37), the new drawings MUST be filed within the THREE MONTH shortened statutory period set for reply in the "Notice of Allowability." Extensions of time may NOT be obtained under the provisions of 37 CFR 1.136 for filing the corrected drawings after the mailing of a Notice of Allowability.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. Claims 1, 2, 4 through 14, and 24 through 26 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The term "a function *h*" renders the claim limitation indefinite. Although the claims are given their broadest reasonable interpretation in light of the specification, limitations from the specification are not read into the claim language. See MPEP § 2106. See also *In re Prater*, 415 F.2d 1393, 1404-05, 162 USPQ 541, 550-551 (CCPA 1969).

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Art Unit: 2131

7. Claims 1 through 4, 14 through 18, 24 through 28, and 31 through 34 are rejected under 35 U.S.C. 102(e) as being anticipated by United States Patent No. 6,317,834 to Gennaro et al., hereinafter Gennaro.

8. The applied reference has a common assignee with the instant application. Based upon the earlier effective U.S. filing date of the reference, it constitutes prior art under 35 U.S.C. 102(e). This rejection under 35 U.S.C. 102(e) might be overcome either by a showing under 37 CFR 1.132 that any invention disclosed but not claimed in the reference was derived from the inventor of this application and is thus not the invention "by another," or by an appropriate showing under 37 CFR 1.131.

9. As per claims 1 and 31, Gennaro teaches a method of processing semiotic data, comprising:

receiving biometric data including a data set P (Figures 1 [block 274], 4a [block 12], 7a [block 752], 10a [blocks 1020], 11 [block 166]; column 1, line 62 to column 2, line 5; column 4, line 64 to column 5, line 1; column 6, lines 4-29; column 9, lines 1-3; column 12, lines 21-24);

selecting a function h , and for at least one of each said data set P to be collected, computing $h(P)$ (Figures 1 [block 276], 4a [block 18], 7a [block 762], 10a [blocks 1040], 11 [block 176]; column 1, line 62 to column 2, line 5; column 5, lines 1-8; column 6, lines 31-44; column 9, lines 1-5; column 12, lines 20-24);

destroying said data set P (column 6, lines 31-44; column 9, lines 1-5); and

storing $h(P)$ in a database, wherein said data set P cannot be extracted from $h(P)$ (Figure 1 [block 280], 4a [block 22], 7a [block 769], 10a [block 1200], 11 [block 184]; column 1, line 62 to column 2, line 5; column 5, lines 1-8; column 6, lines 56-65; column 12, lines 29-31). It is

Art Unit: 2131

inherent to the system of Gennaro to discard the data set P. By discarding of the data set P, or in the case of Gennaro variable S, it removes a possible weakness from the system by removing one of the options needed to authenticate into the system. By storing the data set, it creates the vulnerability of someone hacking into the system and using a copy to spoof a user identity.

10. Regarding claims 2 and 25, Gennaro teaches wherein said semiotic data comprises biometric data (column 4, lines 37-56).

11. Regarding claim 3, Gennaro teaches wherein said function h comprises a secure hash function (Figures 1 [block 276], 4a [block 18], 7a [block 762], 10a [blocks 1040], 11 [block 176]; column 1, line 62 to column 2, line 5; column 5, lines 1-8; column 6, lines 31-44; column 9, lines 1-5; column 12, lines 20-24).

12. Regarding claim 4, Gennaro teaches further comprising:

to determine whether P' is a predetermined subject, comparing h(P) to all available h(P)s to determine whether there is a match (Figures 2 [blocks 284, 288], 3 [block 360], 4b [block 42, 44], 7b [block 790], 10b [block 156]; column 5, lines 17-38; column 5, lines 55-65; column 10, lines 15-21).

13. Regarding claims 14, 16, 18, 26, 28, 32, and 34 Gennaro teaches wherein said data set comprises a personal data set (Figures 4a [block 22], 7a [block 769], 10a [block 1200]; column 6, lines 56-65; column 9, lines 31-46; column 12, lines 29-31).

Art Unit: 2131

14. As per claim 15, Gennaro teaches a method of processing biometric data, comprising:

acquiring unencrypted biometric data including at least one data set P (Figures 1 [block 274], 4a [block 12], 7a [block 752], 10a [blocks 1020], 11 [block 166]; column 1, line 62 to column 2, line 5; column 4, line 64 to column 5, line 1; column 6, lines 4-29; column 9, lines 1-3; column 12, lines 21-24);

encrypting, with one of a secure hash function and an identity function, each said at least one data set acquired; destroying the unencrypted data set P (Figures 1 [block 276], 4a [block 18], 7a [block 762], 10a [blocks 1040], 11 [block 176]; column 1, line 62 to column 2, line 5; column 5, lines 1-8; column 6, lines 31-44; column 9, lines 1-5; column 12, lines 20-24); and

storing each of the at least one encrypted data set in a database (Figure 1 [block 280], 4a [block 22], 7a [block 769], 10a [block 1200], 11 [block 184]; column 1, line 62 to column 2, line 5; column 5, lines 1-8; column 6, lines 56-65; column 12, lines 29-31),

wherein unencrypted biometric data is not available nor retrievable from said data stored in said database (column 6, lines 31-44; column 9, lines 1-5). It is inherent to the system of Gennaro to discard the data set P. By discarding of the data set P, or in the case of Gennaro variable S, it removes a possible weakness from the system by removing one of the options needed to authenticate into the system. By storing the data set, it creates the vulnerability of someone hacking into the system and using a copy to spoof a user identity.

15. As per claims 17 and 33, Gennaro teaches method of extracting components of biometric data which are stable under measurement errors, comprising:

acquiring unencrypted biometric data including at least one data set P (Figures 1 [block 274], 4a [block 12], 7a [block 752], 10a [blocks 1020], 11 [block 166]; column 1, line 62 to

Art Unit: 2131

column 2, line 5; column 4, line 64 to column 5, line 1; column 6, lines 4-29; column 9, lines 1-3; column 12, lines 21-24);

encrypting each said at least one data set acquired to form at least one encrypted data set (Figures 1 [block 276], 4a [block 18], 7a [block 762], 10a [blocks 1040], 11 [block 176]; column 1, line 62 to column 2, line 5; column 5, lines 1-8; column 6, lines 31-44; column 9, lines 1-5; column 12, lines 20-24);

destroying the unencrypted data set P (column 6, lines 31-44; column 9, lines 1-5); and storing each said at least one encrypted data set in a database (Figure 1 [block 280], 4a [block 22], 7a [block 769], 10a [block 1200], 11 [block 184]; column 1, line 62 to column 2, line 5; column 5, lines 1-8; column 6, lines 56-65; column 12, lines 29-31),

wherein unencrypted biometric data is not available nor retrievable from said data stored in said database (column 6, lines 31-44; column 9, lines 1-5). It is inherent to the system of Gennaro to discard the data set P. By discarding of the data set P, or in the case of Gennaro variable S, it removes a possible weakness from the system by removing one of the options needed to authenticate into the system. By storing the data set, it creates the vulnerability of someone hacking into the system and using a copy to spoof a user identity.

16. As per claim 24, Gennaro teaches a system for processing semiotic data, comprising:

means for receiving semiotic data including a data set P (Figures 1 [block 274], 4a [block 12], 7a [block 752], 10a [blocks 1020], 11 [block 166]; column 1, line 62 to column 2, line 5; column 4, line 64 to column 5, line 1; column 6, lines 4-29; column 9, lines 1-3; column 12, lines 21-24);

Art Unit: 2131

means for selecting a function h , and for each said data set P to be collected, computing $h(P)$ (Figures 1 [block 276], 4a [block 18], 7a [block 762], 10a [blocks 1040], 11 [block 176]; column 1, line 62 to column 2, line 5; column 5, lines 1-8; column 6, lines 31-44; column 9, lines 1-5; column 12, lines 20-24);

means for destroying said data set P (column 6, lines 31-44; column 9, lines 1-5); and means for storing $h(P)$ in a database, wherein said data set P cannot be extracted from $h(P)$ (Figure 1 [block 280], 4a [block 22], 7a [block 769], 10a [block 1200], 11 [block 184]; column 1, line 62 to column 2, line 5; column 5, lines 1-8; column 6, lines 56-65; column 12, lines 29-31). It is inherent to the system of Gennaro to discard the data set P . By discarding of the data set P , or in the case of Gennaro variable S , it removes a possible weakness from the system by removing one of the options needed to authenticate into the system. By storing the data set, it creates the vulnerability of someone hacking into the system and using a copy to spoof a user identity.

17. As per claim 27, Gennaro teaches system for verifying biometric data without storing unencrypted biometric data, comprising:

means for acquiring unencrypted biometric data including at least one data set P (Figures 1 [block 274], 4a [block 12], 7a [block 752], 10a [blocks 1020], 11 [block 166]; column 1, line 62 to column 2, line 5; column 4, line 64 to column 5, line 1; column 6, lines 4-29; column 9, lines 1-3; column 12, lines 21-24);

means for encrypting each said at least one data set acquired to form at least one encrypted data set (Figures 1 [block 276], 4a [block 18], 7a [block 762], 10a [blocks 1040], 11

Art Unit: 2131

[block 176]; column 1, line 62 to column 2, line 5; column 5, lines 1-8; column 6, lines 31-44; column 9, lines 1-5; column 12, lines 20-24);

means for destroying the unencrypted data set P (column 6, lines 31-44; column 9, lines 1-5); and

means for storing each said at least one encrypted data set in a database, wherein unencrypted biometric data is not available nor retrievable from said data stored in said database (Figure 1 [block 280], 4a [block 22], 7a [block 769], 10a [block 1200], 11 [block 184]; column 1, line 62 to column 2, line 5; column 5, lines 1-8; column 6, lines 56-65; column 12, lines 29-31). It is inherent to the system of Gennaro to discard the data set P. By discarding of the data set P, or in the case of Gennaro variable S, it removes a possible weakness from the system by removing one of the options needed to authenticate into the system. By storing the data set, it creates the vulnerability of someone hacking into the system and using a copy to spoof a user identity.

Claim Rejections - 35 USC § 103

18. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

19. Claims 5 through 8 are rejected under 35 U.S.C. 103(a) as being obvious over Gennaro in view of United States Patent No. 6,167,518 to Padgett et al., hereinafter Padgett.

20. The applied reference has a common assignee with the instant application. Based upon the earlier effective U.S. filing date of the reference, it constitutes prior art only under 35 U.S.C.

Art Unit: 2131

102(e). This rejection under 35 U.S.C. 103(a) might be overcome by: (1) a showing under 37 CFR 1.132 that any invention disclosed but not claimed in the reference was derived from the inventor of this application and is thus not an invention "by another"; (2) a showing of a date of invention for the claimed subject matter of the application which corresponds to subject matter disclosed but not claimed in the reference, prior to the effective U.S. filing date of the reference under 37 CFR 1.131; or (3) an oath or declaration under 37 CFR 1.130 stating that the application and reference are currently owned by the same party and that the inventor named in the application is the prior inventor under 35 U.S.C. 104, together with a terminal disclaimer in accordance with 37 CFR 1.321(c). For applications filed on or after November 29, 1999, this rejection might also be overcome by showing that the subject matter of the reference and the claimed invention were, at the time the invention was made, owned by the same person or subject to an obligation of assignment to the same person. See MPEP § 706.02(I)(1) and § 706.02(I)(2).

21. Regarding claim 5, Gennaro teaches further comprising:

choosing said function h as the public encryption function corresponding to k (Figures 1 [block 276], 4a [block 18], 7a [block 762], 10a [blocks 1040], 11 [block 176]; column 1, line 62 to column 2, line 5; column 5, lines 1-8; column 6, lines 31-44; column 9, lines 1-5; column 12, lines 20-24).

22. Gennaro does not teach

selecting a private key/public key (K, k) once for all cases; and

one of destroying said private key K and sending said private key K to a trusted party .

23. Padgett teaches:

Art Unit: 2131

selecting a private key/public key (K, k) once for all cases (column 5, lines 5-23); and one of destroying said private key K and sending said private key K to a trusted party (column 5, lines 5-23). It would have been obvious to one of ordinary skill in the art at the time the invention was made to use a private/public key system and only supplying the private key to a trusted third party. One would be motivated to include such a security feature as it would aid in preventing the system from being cracked and a user's identity from being stolen.

24. With regards to claim 6, Gennaro teaches wherein said data set P cannot be extracted from $h(P)$, except by the trusted party (Figures 4b [block 40], 7b [block 788], 10b [block 154]; column 7, lines 22-50; column 10, lines 9-19).

25. With regards to claim 7, Gennaro teaches further comprising:

to determine whether some P' is a predetermined subject, comparing said $h(P)$ to all available $h(P)$ s (Figures 2 [blocks 284, 288], 3 [block 360], 4b [block 42, 44], 7b [block 790], 10b [block 156]; column 5, lines 17-38; column 5, lines 55-65; column 10, lines 15-21); and

determining whether there is a match (Figures 2 [blocks 284, 288], 3 [block 360], 4b [block 42, 44], 7b [block 790], 10b [block 156]; column 5, lines 17-38; column 5, lines 55-65; column 10, lines 15-21).

26. With regards to claim 8, Gennaro teaches wherein the trusted party comprises a panel of members (Figure 11 [blocks 184, 186]; column 14, lines 3-33), and

Art Unit: 2131

wherein a secret is shared among the members so that only at least a predetermined number of panel members can reconstitute the secret in its entirety by putting together their share of the secret (Figure 11 [blocks 184, 186]; column 14, lines 3-33).

27. Claim 9 is rejected under 35 U.S.C. 103(a) as being obvious over Gennaro in view of United States Patent No. 6,363,485 to Adams et al., hereinafter Adams.

28. The applied reference has a common assignee with the instant application. Based upon the earlier effective U.S. filing date of the reference, it constitutes prior art only under 35 U.S.C. 102(e). This rejection under 35 U.S.C. 103(a) might be overcome by: (1) a showing under 37 CFR 1.132 that any invention disclosed but not claimed in the reference was derived from the inventor of this application and is thus not an invention "by another"; (2) a showing of a date of invention for the claimed subject matter of the application which corresponds to subject matter disclosed but not claimed in the reference, prior to the effective U.S. filing date of the reference under 37 CFR 1.131; or (3) an oath or declaration under 37 CFR 1.130 stating that the application and reference are currently owned by the same party and that the inventor named in the application is the prior inventor under 35 U.S.C. 104, together with a terminal disclaimer in accordance with 37 CFR 1.321(c). For applications filed on or after November 29, 1999, this rejection might also be overcome by showing that the subject matter of the reference and the claimed invention were, at the time the invention was made, owned by the same person or subject to an obligation of assignment to the same person. See MPEP § 706.02(l)(1) and § 706.02(l)(2).

29. Regarding claim 9, Gennaro does not teach wherein the data set P is not determined perfectly by its reading,

Art Unit: 2131

wherein each reading gives a number P_i , wherein i is no less than 0, wherein P_0 is for an initial reading, and a secret version of said initial reading is stored after further processing thereof,

wherein reading P_0 is different from P_i for $i > 0$, and the secret version of P_0 is different from the secret version of P_i , such that no identification is possible by a direct comparison of the encrypted data.

30. Adams teaches wherein the data set P is not determined perfectly by its reading,

wherein each reading gives a number P_i , wherein i is no less than 0, wherein P_0 is for an initial reading, and a secret version of said initial reading is stored after further processing thereof (Figure 4 [block 404]; column 4, lines 4-34),

wherein reading P_0 is different from P_i for $i > 0$, and the secret version of P_0 is different from the secret version of P_i , such that no identification is possible by a direct comparison of the encrypted data (Figure 4 [block 404]; column 4, lines 4-34). It would have been obvious to one of ordinary skill in the art at the time the invention was made to record multiple instances of the data set. One would be motivated to record multiple instances of the data set as it would account for any irregularities that may occur. By taking into account that irregularities would occur, multiple instances or an average of the data set would serve as a better function in identifying a person.

31. Claims 10 through 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gennaro in view of Adams as applied to claim 9 above, and further in view of United States Patent No. 6,487,662 to Kharon et al., hereinafter Kharon.

32. With regards to claim 10, Gennaro and Adams do not teach:

Art Unit: 2131

extracting sub-collections S_j from the collection of data in data set P; and
encrypting a predetermined number of such sub-collections such that at least one of the sub-collections is reproduced exactly with a predetermined probability.

33. Kharon teaches further comprising:

extracting sub-collections S_j from the collection of data in data set P (Figure 6 [block 340]; column 13, lines 43-67); and

encrypting a predetermined number of such sub-collections such that at least one of the sub-collections is reproduced exactly with a predetermined probability (Figure 6 [block 347]; column 13, lines 43-67). It would have been obvious to one of ordinary skill in the art at the time the invention was made to sample a smaller section of the data set. One would be motivated to do because there is a better probability that a smaller area is less likely to change, therefore making it more difficult for someone to steal someone's identification.

34. Concerning claim 11, Gennaro and Adams do not teach:

comparing encrypted versions of the sub-collections S_j with those data stored in said database,

wherein if one or more of the sub-collection S_j matches with said data, then verification is deemed to have occurred.

35. Kharon teaches further comprising:

comparing encrypted versions of the sub-collections S_j with those data stored in said database (Figure 6 [blocks 345, 347]; column 13, lines 43-67; column 14, lines 28-39; column 15, lines 42-55),

wherein if one or more of the sub-collection S_j matches with said data, then verification is deemed to have occurred (Figure 6 [blocks 345, 347]; column 13, lines 43-67; column 14, lines 28-39; column 15, lines 42-55). It would have been obvious to one of ordinary skill in the art at the time the invention was made to sample a smaller section of the data set. One would be motivated to do because there is a better probability that a smaller area is less likely to change, therefore making it more difficult for someone to steal someone's identification.

36. Concerning claim 12, Gennaro teaches further comprising:

encrypting all such modified data, and comparing said encrypted modified data to data stored in said database (Figures 1 [block 276], 4a [block 18], 7a [block 762], 10a [blocks 1040], 11 [block 176]; column 1, line 62 to column 2, line 5; column 5, lines 1-8; column 6, lines 31-44; column 9, lines 1-5; column 12, lines 20-24).

37. Gennaro does not teach:

each time a P_i , with $i > 0$, is read, computing all possible predetermined size variations of P_i which correspond to an acceptable predetermined imprecision of the reading.

38. Adams teaches:

each time a P_i , with $i > 0$, is read, computing all possible predetermined size variations of P_i which correspond to an acceptable predetermined imprecision of the reading (Figure 4 [block 404]; column 4, lines 4-34). It would have been obvious to one of ordinary skill in the art at the time the invention was made to record multiple instances of the data set. One would be motivated to record multiple instances of the data set as it would account for any irregularities that may occur. By taking into account that irregularities would occur, multiple instances or an average of the data set would serve as a better function in identifying a person.

39. Concerning claim 13, Gennaro teaches wherein for a plurality of users of the same biometric information, said biometric information is encrypted differently for each user (Figure 3 [block 330]; column 5, lines 47-54).

40. Claims 19, 20, 21, 29, 30, and 35, and 36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gennaro in view of Kharon.

41. As per claims 19, 29, and 35, Gennaro teaches a method of extracting components of biometric data which are stable under measurement errors, comprising:

acquiring unencrypted biometric data including at least one data set P (Figures 1 [block 274], 4a [block 12], 7a [block 752], 10a [blocks 1020], 11 [block 166]; column 1, line 62 to column 2, line 5; column 4, line 64 to column 5, line 1; column 6, lines 4-29; column 9, lines 1-3; column 12, lines 21-24);

encrypting each said at least one data set acquired to form at least one encrypted data set (Figures 1 [block 276], 4a [block 18], 7a [block 762], 10a [blocks 1040], 11 [block 176]; column 1, line 62 to column 2, line 5; column 5, lines 1-8; column 6, lines 31-44; column 9, lines 1-5; column 12, lines 20-24);

destroying the unencrypted data set P (column 6, lines 31-44; column 9, lines 1-5); and

storing each said at least one encrypted data set in a database, wherein unencrypted biometric data is not available nor retrievable from said data stored in said database (Figure 1 [block 280], 4a [block 22], 7a [block 769], 10a [block 1200], 11 [block 184]; column 1, line 62 to column 2, line 5; column 5, lines 1-8; column 6, lines 56-65; column 12, lines 29-31).

42. Gennaro does not teach:

Art Unit: 2131

extracting sub-collections S_j from the collection of data in said data set P; and

encrypting a predetermined number of such sub-collections such that at least one of the sub-collections is reproduced exactly with a predetermined probability.

43. Kharon teaches:

extracting sub-collections S_j from the collection of data in said data set P (Figure 6 [block 340]; column 13, lines 43-67); and

encrypting a predetermined number of such sub-collections such that at least one of the sub-collections is reproduced exactly with a predetermined probability (Figure 6 [block 347]; column 13, lines 43-67). It would have been obvious to one of ordinary skill in the art at the time the invention was made to sample a smaller section of the data set. One would be motivated to do because there is a better probability that a smaller area is less likely to change, therefore making it more difficult for someone to steal someone's identification.

44. Claims 20, 21, 30, and 36 are rejected for similar reasons as stated above.

45. Claims 22 and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gennaro in view of Kharon as applied to claim 21 above, and further in view of Adams.

46. Claims 22 and 23 are rejected for similar reasons as stated above.

Double Patenting

47. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. See *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed.

Art Unit: 2131

Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970);and, *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

48. A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent is shown to be commonly owned with this application. See 37 CFR 1.130(b).

49. Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

50. Claims 1 through 36 are rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1 through 22 of U.S. Patent No. 6,317,834. Although the conflicting claims are not identical, they are not patentably distinct from each other because there are minute and obvious type differences. For example, claim 5 of the instant application discloses a private key/public key set, while the patent discloses a symmetric key system, not a public key system.

Claim Objections

51. Claims 2 and 3 are objected to under 37 CFR 1.75(c), as being of improper dependent form for failing to further limit the subject matter of a previous claim. Applicant is required to cancel the claim(s), or amend the claim(s) to place the claim(s) in proper dependent form, or rewrite the claim(s) in independent form.

Art Unit: 2131

52. Claim 25 is objected to because of the following informalities: it depends from itself. Appropriate correction is required. For the purposes of examination, the Examiner will assume that claim 25 depends from claim 24.

53. Claim 34 is objected to under 37 CFR 1.75(c), as being of improper dependent form for failing to further limit the subject matter of a previous claim. Applicant is required to cancel the claim(s), or amend the claim(s) to place the claim(s) in proper dependent form, or rewrite the claim(s) in independent form. For the purposes of examination, the Examiner will assume that claim 34 depends from claim 33.

Conclusion

54. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

55. The following patents are cited to further show the state of the art with respect to biometric identification, such as:

United States Patent No. 5,790,668 to Tomko, which is cited to show a method for securely handling data in a database of biometrics.

United States Patent No. 6,167,517 to Gilchrist et al., which is cited to show trusted biometric client authentication.

United States Patent No. 6,167,518 to Padgett et al., which is cited to show a digital signature based on biological indicia.

United States Patent No. 6,038,315 to Strait et al., which is cited to show a method and system for normalizing biometric variations to authenticate users from a public database.

United States Patent No. 4,991,205 to Lemelson, which is cited to show a personal identification system.

United States Patent No. 4,993,068 to Piosenka, which is cited to show an unforgeable personal identification system.

United States Patent No. 5,991,408 to Pearson et al., which is cited to show an identification method using biometric measurements.

United States Patent No. 6,535,878 to Padgett et al., which is cited to show a digital signature based on biological indicia.


56. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian La Forgia whose telephone number is (703) 305-7704. The examiner can normally be reached on Monday thru Thursday 7-5.

57. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (703) 305-9648. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

58. Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

Christian LaForgia
Patent Examiner
Art Unit 2131

clf


AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100